Glasgow Mathematical Journal (2025), **67**, pp. 245–268
doi:10.1017/S0017089524000351

Glasgow Mathematical Journal

RESEARCH ARTICLE

Optimal linear sofic approximations of countable groups

Keivan Mallahi-Karai[1] and Maryam Mohammadi Yekta[2]

[1]Constructor University, Bremen, Germany
[2]University of Waterloo, Ontario, Canada
Corresponding author: Keivan Mallahi-Karai; Email: kmallahikarai@constructor.university

Received: 12 April 2024; **Revised:** 25 November 2024; **Accepted:** 3 December 2024; **First published online:** 24 January 2025

Keywords: linear sofic groups; metric approximations; sofic groups

2020 Mathematics Subject Classification: *Primary* - 60B15, 20E26; *Secondary* - 60G50

Abstract

Let G be a group. The notion of linear sofic approximations of G over an arbitrary field F was introduced and systematically studied by Arzhantseva and Păunescu [3]. Inspired by one of the results of [3], we introduce and study the invariant $\kappa_F(G)$ that captures the quality of linear sofic approximations of G over F. In this work, we show that when F has characteristic zero and G is linear sofic over F, then $\kappa_F(G)$ takes values in the interval $[1/2, 1]$ and $1/2$ cannot be replaced by any larger value. Further, we show that under the same conditions, $\kappa_F(G) = 1$ when G is torsion-free. These results answer a question posed by Arzhantseva and Păunescu [3] for fields of characteristic zero. One of the new ingredients of our proofs is an effective non-concentration estimates for random walks on finitely generated abelian groups, which may be of independent interest.

1. Introduction

Let $\mathcal{G} = \{(G_n, \mathrm{dist}_n)\}_{n\geq 1}$ be a family of groups, each equipped with a bi-invariant bounded metric. Bi-invariance means that for every $x, y, g_1, g_2 \in G_n$, we have the equality:

$$\mathrm{dist}_n(g_1 x g_2, g_1 y g_2) = \mathrm{dist}_n(x, y)$$

A $\mathcal{G}$-approximation of a countable group G consists of an increasing sequence $(n_k)_{k\geq 1}$ of positive integers and a sequence $(\phi_k)_{k\geq 1}$ of maps:

$$\phi_k : G \to G_{n_k}, \quad k \geq 1$$

satisfying the following two properties:

1. (Asymptotic homomorphism) For all $g, h \in G$, one has
$$\lim_{k\to\infty} \mathrm{dist}_{n_k}(\phi_k(gh), \phi_k(g)\phi_k(h)) = 0.$$
2. (Uniform injectivity) There exists $\kappa > 0$ such that for all $g \in G \setminus \{e_\Gamma\}$,
$$\limsup_{k\to\infty} \mathrm{dist}_{n_k}\left(\phi_k(g), e_{G_{n_k}}\right) \geq \kappa.$$

We will then also say that G is κ-approximable by $\mathcal{G}$. Perhaps the most prominent and well-studied classes of approximable groups are the sofic and hyperlinear groups, which correspond, respectively, to approximation by the family of symmetric groups equipped with the normalized Hamming distance and the family of unitary groups equipped with normalized Hilbert–Schmidt distance. The class of sofic groups was introduced by Gromov in connection with the so-called Gottschalk surjunctivity conjecture [11], while the terminology is due to Weiss [23]. Hyperlinear groups first appeared in the context of Conne's embedding conjecture. The term hyperlinear was coined by Rădulescu [21]. Sofic groups are shown to be hyperlinear [[8], Theorem 2], It is unknown whether every group is sofic, or even hyperlinear.

© The Author(s), 2025. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

The class of linear sofic groups over an arbitrary field was introduced by Arzhantseva and Păunescu [[3], Definition 4.1 and the paragraph following Definition 4.2] who proved fundamental results about this class of groups. This mode of approximation defining linear sofic groups uses general linear groups (over a general field F fixed in the discussion) as target groups, while the metric is defined using the normalized rank. In this regards, linear sofic groups provide a hybrid form of approximation.

In order to define this metric, let F be a field. For $d \times d$ matrices $A, B \in \mathrm{GL}_d(F)$, we define

$$\rho_d(A, B) := \frac{1}{d}\mathrm{rank}(A - B).$$

The following definition of linear sofic groups will be more convenient for our purpose. The equivalence of two definitions is proven in [[3], Proposition 4.4].

Definition 1.1. *Let F be a field, G a countable group and $0 < \kappa \leq 1$. We say that G is κ-linear sofic over F if for every finite set $S \subseteq G$ and every $\delta > 0$ and every $0 \leq \kappa' < \kappa$, there exists $d \geq 1$ and a map $\phi : S \to \mathrm{GL}_d(F)$ satisfying the following two properties:*

(AH) For all $g, h, gh \in S$, one has $\rho_d(\phi(gh), \phi(g)\phi(h)) < \delta$.
(D) For all $g \in S \setminus \{e\}$, $\rho_d(\phi(g), \mathrm{Id}) \geq \kappa'$.

Such a map is called an (S, δ, κ')-map. Roughly speaking, (AH) guarantees that ϕ is *almost* a homomorphism, while (D) shows that distinct elements are separated out. Following [3], we say that G is linear sofic over F if it is κ-linear sofic for some $\kappa > 0$. It is clear that if $\kappa_1 < \kappa_2$, then every κ_2-linear sofic group is κ_1-linear sofic. For a countable group G, we write

$$\kappa_F(G) = \sup\{\kappa \geq 0 : G \text{ is } \kappa\text{-linear sofic over } F\} \in (0, 1].$$

Note that whenever G is not κ-linear sofic over F for any $\kappa > 0$, we define $\kappa_F(G)$ to be zero.

Remark 1.2. *The notion of metric approximation can also be defined using the notion of metric ultraproducts. This alternative definition allows one to avoid limiting processes that require passing to subsequences and thereby simplifies certain arguments, see [3] for examples. Since this point of view will not provide us with any special advantages, we will not use this definition.*

1.1. The amplification argument

Let $\mathcal{G} = \{(G_n, \mathrm{dist}_n)\}_{n\geq 1}$ be as above, and assume that the diameter of G_n with respect to dist_n is normalized to be 1. It is natural to ask whether a κ-approximable group for some $\kappa > 0$ is always 1-approximable. Elek and Szabó [8] proved that this is the case for sofic groups. A similar statement (with a modified proof) holds for hyperlinear groups. Note that this implies that analogously defined κ_{sofic} and $\kappa_{\mathrm{hyperlinear}}$ can only take values in the set $\{0, 1\}$, and the long-standing open question asking whether all groups are sofic is equivalent to $\kappa_{\mathrm{sofic}}(G) = 1$ for all groups G.

Let us recall that both proofs are based on a basic tool, often referred to as *amplification*, which uses the identity:

$$\mathrm{tr}(a \otimes b) = \mathrm{tr}(a)\mathrm{tr}(b). \tag{1.1}$$

for matrices a and b. This identity allows one to show that there exists a function $f : (0, 1) \to (0, 1)$ such that if one starts with a map $\phi : S \to \mathsf{S}_n$ with $\mathrm{dist}_{\mathrm{Hamm}}(\phi(g), e) \geq \beta$, then the tensor power $\phi^{\otimes 2} : S \to \mathsf{S}_{n\times n}$ defined by $\phi^{\otimes 2}(g)(i, j) = (\phi(g)(i), \phi(g)j)$ satisfies $\mathrm{dist}_{\mathrm{Hamm}}(\phi^{\otimes 2}(g), e) \geq f(\beta)$. Moreover, starting from any β, the sequence of iterates $f^{(n)}(\beta)$ converges to 1. Hence, by iterating the tensor power operation, one can arrive at arbitrarily well sofic approximation. The case of hyperlinear groups is dealt with in a similar fashion. As it was observed in [3], (1.1) does not have an analog for linear sofic approximations. In [3], Arzhantseva and Păunescu invented a new amplification argument to prove that every linear sofic

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

group is $1/4$-linear sofic. A particularly innovative aspect of this argument is that it tracks two different quantities that when coupled together can be used to control the distance to the identity. Then using clever properties of ranks of tensor powers, they prove that this amplification argument works. The question of whether the constant $1/4$ can be improved is left open in [3]. We will build upon their work to answer this question in the case of fields of characteristic zero.

1.2. Statement of results

In this paper, we will address the question of optimality of linear sofic approximations. The main results of this paper is the theorem below.

Theorem A. *Let G be a countable linear sofic group over $\mathbb{C}$. Then*

1. *If G is torsion-free, then G is 1-linear sofic over $\mathbb{C}$.*
2. *Unconditionally, G is $1/2$-linear sofic over $\mathbb{C}$. Moreover, the constant $1/2$ cannot be improved.*

Note that the assertion in Theorem A is in stark contrast with the case of sofic and hyperlinear groups. An interesting observation in [3] (see the paragraph before Proposition 5.12) is that the amplification argument does not *see* the interaction between group elements and will equally work for a subset of a group. Theorem A, however, shows that the optimal constant does indeed depend on the group structure and can even change by passing to a subgroup of finite index.

Remark 1.3. *Although we stated Theorem A over $\mathbb{C}$, one can easily see that it implies the same statement over all fields of characteristic zero; see Remark 5.1. However, an important part of the argument that is based on Lemma 4.2 does not work when F has positive characteristic. See Remark 5.2 for more details. Henceforth, we write κ instead of $\kappa_{\mathbb{C}}$.*

We briefly outline the proof of Theorem A, which is following the main strategy of [3]. Given a finite subset $S \subseteq G$ and $\delta_0 > 0$, we start with an $(S, \delta_0, 0.24)$-map ϕ_0 (in the sense of Definition 1.1) provided by [3]. Using a sequence of functorial operations (see 2.1 for definitions), we replace ϕ_0 with an $(S, \delta_0, 0.23)$-map which has the additional property that for every $g \in S$, at least $1/100$ of eigenvalues of matrix $\phi(g)$ are 1. We will then show that the rank of tensor powers of $\phi(g)$ are controlled by the return probability of a certain random walk on a finitely generated subgroup of $\mathbb{C}^*$. We will establish required *effective* non-concentration estimates in Theorem 3.9. This part of proof uses a variety of tools ranging from Fourier analysis to additive combinatorics. Let us note that the effectiveness of these bounds is a key element of the proof: as the asymptotic homomorphism condition (AH) deteriorates after every iteration of tensor power, we need to know in advance the number of required iterations so that we can start with an appropriate δ_0. The counter-intuitive move of adding ones as eigenvalues is needed for this purpose. When $\phi_0(g)$ is close to unipotent, this argument completely breaks down. In this case, again using the method of [3], we will instead show the normalized number of Jordan block of tensor powers tends to zero with an effective bound for speed. This is carried out in Theorem 4.1 by translating the problem to estimating integrals of certain trigonometric sums. In summary, our proof can be viewed as a version of amplification argument where we use additional functors in the process.

Another result of this paper involves determining $\kappa(G)$ for finite groups.

Theorem B. *Let G be a finite group.*

1. *There exists a finite-dimensional linear representation $\psi : G \to \mathrm{GL}_d(\mathbb{C})$ of G such that*
$$\kappa(G) = \min_{g \in G} \rho_d(\psi(g), \mathrm{Id}).$$
In particular, $\kappa(G)$ is a rational number.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

2. $\kappa(G) = 1$ *iff* G *has a fixed-point free complex representation.*
3. *Let* $\mathbb{Z}_p$ *denote the cyclic group of order* p*. For prime* p *and* $n \geq 2$*, we have*

$$\kappa(\mathbb{Z}_p^n) = \frac{p^n - p^{n-1}}{p^n - 1}.$$

In particular, $\kappa(\mathbb{Z}_2^n) \to 1/2$ *as* $n \to \infty$*.*

One of the main ingredients in the proof of Theorem B is the notion of stability. Broadly described, stability of a group in a mode of metric approximation demands that almost representations be small deformations of exact representations. Finite groups are easily seen to enjoy this property with respect to linear sofic approximations, see Proposition 6.2. Once this is established, the problem reduces to representation theory of finite groups. Proof of Part (a) of Theorem B is based on the simplex method in linear programming. Part (3) implements this for groups $\mathbb{Z}_p^n$, $n \geq 2$. We finally remark that all finite groups to which (2) of Theorem A applies have been classified by Joseph Wolf [24]. They include groups such as $\mathrm{PSL}_2(\mathbb{F}_5)$. The next result establishes the value of $\kappa_F(G)$ for certain classes of groups over fields of positive characteristic.

Theorem C. *Let* F *be a field of characteristic* p*, and let* G *be a finite group such that* p *is the smallest prime dividing* $|G|$*. Then*

$$\kappa_F(G) = 1 - \frac{1}{p}.$$

One of the problems posed in [3] is whether the notions of linear sofic approximation over $\mathbb{C}$ and $\mathbb{F}_p$ are equivalent. Theorem B and Theorem C together show that in general the values of $\kappa_{\mathbb{C}}(G)$ and $\kappa_{\mathbb{F}_p}(G)$ need not coincide for a finite group G. This may be viewed as a quantitative reason for the difficulty of the problem of equivalence. We note that quantitative approaches to other metric approximations have also been considered before, see [1].

This paper is organized as follows: in Section 2, we will collect basic facts related to the rank metric, and basic theory of random walks on abelian groups and explain how they relate to our question. In Section 3, we prove various non-concentration estimates for random walks on abelian groups. Section 4 contains the proof of Theorem 4.1, involving matrices in Jordan canonical form. These ingredients are put together in Section 5 to prove Theorem A, except for the optimality claim. The optimality, as well as the proof of Theorems B and C, are discussed in Section 6.

2. Preliminaries and notation

In this section, we will set some notation and gather a number of basic facts needed in the rest of the paper. We will denote the group of invertible $d \times d$ matrices over the field $\mathbb{C}$ by $\mathrm{GL}_d(\mathbb{C})$. This space can be turned into a metric space by defining for $A, B \in \mathrm{GL}_d(\mathbb{C})$:

$$\rho_d(A, B) = \frac{\mathrm{rank}(A - B)}{d}.$$

We will often suppress the subscript d and simply write $\rho(A, B)$. Every $A \in \mathrm{GL}_d(\mathbb{C})$ has d eigenvalues $\lambda_1, \ldots, \lambda_d$, each counted with multiplicity. We write

$$\mathbf{m}_1(A) = \frac{1}{d}\#\{1 \leq i \leq d : \lambda_i = 1\}.$$

For $j \geq 1$, let us denote by W_j the set of all j-th roots of unity in $\mathbb{C}$. It will later be convenient to consider the following quantity:

$$\mathbf{m}^{\leq r}(A) = \frac{1}{d}\#\left\{1 \leq i \leq d : \lambda_i \in \bigcup_{j=1}^{r} W_j\right\}.$$

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

The number of Jordan blocks of A (in its Jordan canonical form) will be denoted by $\mathbf{j}(A)$. The number of Jordan blocks corresponding with 1 on the diagonal will be denoted by $\mathbf{j}_1(A)$. Note that

$$\mathbf{j}_1(A) = \dim \ker (A - \mathrm{Id}) = (1 - \rho(A, \mathrm{Id}))d.$$

The following lemma plays a key role in the arguments used in [3]:

Lemma 2.1 ([3]). *For every $A \in \mathrm{GL}_d(\mathbb{C})$, we have*

$$\rho(A, \mathrm{Id}) \geq \max (1 - \mathbf{m}_1(A), 1 - \mathbf{j}(A)).$$

The next lemma will be essential for tracking the multiplicity of eigenvalue 1 in tensor powers of a matrix A:

Lemma 2.2 ([3], Lemma 5.1). *Suppose that $\{\lambda_1, \ldots, \lambda_d\}$ is the set of eigenvalues of a $d \times d$ complex matrix A, each counted with multiplicity. Then, for $k \geq 1$ the set of eigenvalues of $A^{\otimes k}$ counted with multiplicity is given by:*

$$\left\{\lambda_{i_1} \cdots \lambda_{i_k} : 1 \leq i_j \leq d, \quad 1 \leq j \leq k\right\}.$$

Proof. There exists $P \in \mathrm{GL}_d(\mathbb{C})$ such that $P^{-1}AP$ is upper-triangular. Hence, without loss of generality, we can assume that A is upper-triangular with diagonal entries $\lambda_1, \ldots, \lambda_d$. It is easy to see that $A^{\otimes k}$ will be upper-triangular in an appropriate ordering of the bases, with diagonal entries given by the list above. Special case $k = 2$ is dealt with in Lemma 5.1 of [3]. □

2.1. Three functorial operations

Let us now consider three functorial operations that can be applied to a family of matrices in $\mathrm{GL}_d(\mathbb{C})$. These will be used to replace an (S, δ, κ)-map by an (S, δ', κ')-map, which has some better properties. An alternative point of view is that each operation can be viewed as post-composition of the initial map by a representation of GL_n.

1. (Tensors) Consider the representations
$$\Psi_{T,m} : \mathrm{GL}_d(\mathbb{C}) \to \mathrm{GL}_{d^m}(\mathbb{C}), \quad A \mapsto A \otimes \cdots \otimes A,$$
where m denotes the number of tensors. We will denote $\Psi_{T,m}(A)$ by $\mathsf{T}^m A$.
2. (Direct sums) For $m \geq 1$, let
$$\Psi_{S,m} : \mathrm{GL}_d(\mathbb{C}) \to \mathrm{GL}_{md}(\mathbb{C}), \quad A \mapsto A \oplus \cdots \oplus A,$$
where the number of summands is m. Instead of $\Psi_{S,m}(A)$, we write $\mathsf{S}^m A$.
3. (Adding Identity) For $m \geq 0$, consider the representation
$$\Psi_{I,m} : \mathrm{GL}_d(\mathbb{C}) \to \mathrm{GL}_{m+d}(\mathbb{C}), \quad A \mapsto A \oplus \mathrm{Id}_m,$$
where Id_m is the identity matrix of size m. We write $\mathsf{I}^m A$ for $\Psi_{I,m}(A)$.

Lemma 2.3. *Let A and B be $d \times d$ matrices. Then for $m, n \geq 1$ we have*

1. $\mathbf{m}_1(\mathsf{I}^{md}\mathsf{S}^n A) = \mathbf{m}_1(A) + \frac{m}{n}$.
2. $\rho(\mathsf{I}^{md}\mathsf{S}^n A, \mathsf{I}^{md}\mathsf{S}^n B) \leq \rho(A, B)$.
3. $\rho(\mathsf{I}^{md}\mathsf{S}^n A, \mathrm{Id}) = \frac{n}{n+m}\rho(A, \mathrm{Id})$.

Proof. Parts (1) and (2) are straightforward computations. For (3) note that

$$\dim (\ker (\mathsf{I}^{md}\mathsf{S}^n A - \mathsf{I}^{md}\mathsf{S}^n \mathrm{Id})) = n \dim \ker (A - \mathrm{Id}) + md.$$

The claim follows by a simple computation. □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Proposition 2.4. *Let G be a linear sofic group. Then for every finite $S \subseteq G$, $\delta > 0$, and $\kappa < 0.24$, there exists an (S, δ, κ)-map ϕ such that $\mathbf{m}_1(\phi(g)) \geq 0.01$ for all $g \in S \setminus \{e\}$.*

Proof. We know from [3] that $\kappa(G) \geq 1/4$. Since $\kappa + 0.01 < 0.25 \leq \kappa(G)$, there exists a $(S, \epsilon, 0.01 + \kappa)$-map, which we denote by ϕ_0. Set $\phi = \mathsf{I}^d\mathsf{S}^{100}\phi_0$. By Lemma 2.3, we have $\mathbf{m}_1(\phi(g)) \geq 0.01$. Moreover, for every $g \in S \setminus \{e\}$ we have

$$\rho(\phi(g), \mathrm{Id}) \geq \frac{100}{101}(\kappa + 0.01) \geq \kappa.$$

□

Lemma 2.5. *Let A and B be $d \times d$ matrices. Then $\rho(\mathsf{T}^n A, \mathsf{T}^n B) \leq n\rho(A, B)$.*

Proof. For $n = 2$, we have $A \otimes A - B \otimes B = A \otimes (A - B) + (A - B) \otimes B$. The claim follows from [[3], Proposition 5] and the triangle inequality. The general case follows by a simple inductive argument. □

2.2. Preliminaries from probability theory

It will be convenient to reinterpret Lemma 2.2 in a probabilistic language. Let $(\Lambda, +)$ be a countable abelian group with the neutral element denoted by 0. By a probability measure on Λ, we mean a map $\mu : \Lambda \to [0, 1]$ such that $\sum_{a\in\Lambda} \mu(a) = 1$. We will then write $\mu = \sum_{a\in\Lambda} \mu(a)\delta_a$. For $B \subseteq \Lambda$, we define $\mu(B) = \sum_{a\in B} \mu(a)$. We say that μ is finitely supported if there exists a finite set $B \subseteq \Lambda$ such that $\mu(B) = 1$. The smallest set with this property is called the support of μ. Probability measures considered in this paper are finitely supported.

The convolution of probability measures measures μ_1 and μ_2 on Λ is the probability measure defined by:

$$(\mu_1 * \mu_2)(a) = \sum_{a_1+a_2=a} \mu_1(a_1)\mu_2(a_2).$$

One can see that the convolution is commutative and associative. The k-th convolution power of μ will be denoted by $\mu^{(k)}$. Given a probability measure μ on the group A, the μ-random walk on Λ (or the random walk governed by μ) is the random process defined as follows. Let $(X_k)_{k\geq 1}$ be a sequence of independent random variables, where the law of X_i is μ. Define the process $(S_k)_{k\geq 0}$ by $S_0 = 0$ and $S_k = X_1 + \cdots + X_k$. It is easy to see that the law of X_k is $\mu^{(k)}$. We will use the notation $\mathbf{P}[E]$ to denote the probability of an event E. Similarly, $\mathbf{E}[X]$ denotes the expected value of a random variable X.

Given $A \in \mathrm{GL}_d(\mathbb{C})$ with eigenvalues $\lambda_1, \ldots, \lambda_d$, define the probability measure on $\mathbb{C}$:

$$\xi_A := \frac{1}{d}\sum_{i=1}^{d} \delta_{\lambda_i}.$$

Proposition 2.6. *Let A be a $d \times d$ invertible complex matrix. Then*

1. *ξ_A is a finitely supported probability measure on the multiplicative group $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$.*
2. *$\xi_A(1) = \mathbf{m}_1(A)$.*
3. *For all integer $k \geq 1$, we have*

$$\xi_{\mathsf{T}^k(A)} = (\xi_A)^{(k)}.$$

Proof. Parts (1) and (2) follow from the definition of ξ_A. Part (3) is an immediate corollary of Lemma 2.2. □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

3. Effective non-concentration bounds on abelian groups

This section is devoted to proving effective non-concentration bounds for random walks on abelian groups. We will use the additive notation in most of this section. However, we will eventually apply these results to subgroups of the multiplicative group of nonzero complex numbers. Let ν be a finitely supported probability measure on a finitely generated abelian group Λ. Our goal is to prove effective upper bounds for the return probability $\nu^{(n)}(0)$.

Lemma 3.1. *Let ν be a finitely supported probability measure on $\mathbb{Z}^d$ such that $\beta \leq \nu(0) \leq 1-\beta$ for some $0 < \beta < 1/2$. Then*

$$\nu^{(n)}(0) \leq \frac{C}{\sqrt{\beta n}}$$

where C is an absolute constant.

Note that the key aspect of Lemma 3.1 is that the decay rate is controlled only by β without no further assumption on the distribution of ν. This fact will be crucial in our application. The proof of Lemma 3.1 is based on a non-concentration estimate in classical probability theory. Before stating the theorem, we need a few definitions. The concentration function $Q(X, \lambda)$ of a random variable X is defined by:

$$Q(X, \lambda) = \sup_{x \in \mathbb{R}} \mathbf{P}[x \leq X \leq x + \lambda], \quad \lambda \geq 0.$$

We will use a theorem of Rogozin [20], which generalizes a special case due to Kolmogorov[13]. Our statement of the theorem is taken from [[9], Theorem 1], where a new proof using Fourier analysis is given. A variation of this proof can also be found in [[19], Chapter].

Theorem 3.2 (Rogozin). *Suppose $X_1, \ldots, X_n$ are independent random variables and $S_n = X_1 + \cdots + X_n$. Then for every nonnegative $\lambda_1, \ldots, \lambda_n \leq L$, we have*

$$Q(S_n, L) \leq C\, L \left(\sum_{k=1}^{n} \lambda_k^2 (1 - Q(X_k, \lambda_k)) \right)^{-1/2},$$

where C is an absolute constant.

Proof of Lemma 3.1. Let $\iota : \mathbb{Z}^d \to \mathbb{R}$ denote an embedding of $\mathbb{Z}^d$ into $\mathbb{R}$ as an abelian group. Let ν' denote the push-forward of ν which is a finitely supported probability measure defined by $\nu'(x) = \nu(\iota^{-1}(x))$ for every $x \in \mathbb{R}$. Let $X_1, \ldots, X_n$ be independent identically distributed random variables with distribution ν'. Then by choosing all λ_i equal to $\lambda > 0$, we obtain

$$\mathbf{P}[S_n = 0] \leq C(n(1 - Q(X_1, \lambda))^{-1/2}.$$

Letting $\lambda \to 0$ we obtain $\nu'^{(n)}(0) = \mathbf{P}[S_n = 0] \leq C(n(1-q))^{-1/2}$ where $q = \max_{x \in \mathbb{R}} \mathbf{P}[X_i = x]$. Since $\nu'(0) = \nu(0) \geq \beta$, we have $\nu'(x) \leq 1 - \beta$ for all $x \in \mathbb{R} \setminus \{0\}$. Since $\nu(0) \leq 1 - \beta$, we have $q \leq 1 - \beta$. The claim follows by noticing that $\nu^{(n)}(0_{\mathbb{Z}_d}) = \nu'^{(n)}(0_{\mathbb{R}})$. □

Remark 3.3. *It might be tempting to expect a similar upper bound for $\nu^{(n)}(0)$ under the weaker assumption that $\nu(0) \leq 1 - \beta$. This is, however, not true. To see this, consider the probability measure ν_k with $\nu_k(1) = 1 - \frac{1}{k}$ and $\nu_k(-k) = \frac{1}{k}$. Although $\nu_k(0) = 0$, we have for all $k \geq 1$ $\nu_k^{(k+1)}(0) = \frac{k+1}{k}(1 - \frac{1}{k})^k \approx 1/e$.*

We will now consider a variant of Lemma 3.1 for finite cyclic groups $\mathbb{Z}_N$. In this case, the uniform measure is the stationary measure and hence $\nu^n(0)$ (under irreducibility assumptions) will converge to $1/N$ as $n \to \infty$. Note, however, that the random walk and its frequency of visits to zero can be bounded

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

by how much the measure is supported on small subgroups. The next lemma provides an effective upper bound for $\nu^{(n)}(0)$ only depending on the mass given to elements of small order.

Lemma 3.4 (Non-concentration for random walks on cyclic groups). *Let ν be a probability measure on $\mathbb{Z}_N$. Further, suppose that for some $0 < \beta \leq 1/2$ and positive integer $r > 1$ the following hold:*

1. *$\beta \leq \nu(0) \leq 1 - \beta$.*
2. *For every subgroup $H \leq \mathbb{Z}_N$ with $|H| \leq r$, we have $\nu(H) \leq 1 - \beta$.*

Then for all $n \geq 1$, we have

$$\nu^{(n)}(0) \leq \frac{1}{r} + \frac{C'}{\sqrt{\beta n}} + e^{-n\beta/2}.$$

where C' is an absolute constant.

The following proof is an adaptation of the proof of Littlewood-Offord estimate [[18], Theorem 6.3]. This theorem is proven under different conditions, where instead of condition (2), a stronger assumption on the measure of all subgroups is imposed.

The proof uses the Fourier transform of measure and some of Let ν be a probability measure on $\mathbb{Z}_N$. Write $e_N(x) = \exp(2\pi ix/N)$ for $x \in \mathbb{Z}_N$. The following basic property of e_N is used several times in the sequel. For each $a \in \mathbb{Z}_n$, we have $\sum_{x\in\mathbb{Z}_n} e_N(ax)$. We will define the (Fourier) transform $\widehat{\nu}:\mathbb{Z}_N \to \mathbb{C}$ by:

$$\widehat{\nu}(t) := \sum_{a\in\mathbb{Z}_N} \nu(a) e_N(at).$$

Lemma 3.5. *Let ν be a probability measure on $\mathbb{Z}_N$. Then we have*

1. *$\widehat{\nu}(0) = 1$.*
2. *For all $n \geq 1$, we have $\widehat{\nu^{(n)}} = (\widehat{\nu})^n$.*
3. *$\nu(0) = \frac{1}{N} \sum_{t\in\mathbb{Z}_N} \widehat{\nu}(t)$.*

Proof. Part (1) is clear. For (2), suppose that ν_1 and ν_2 are two probability measures on $\mathbb{Z}_N$. Then we have

$$\begin{aligned}
\widehat{\nu_1 * \nu_2}(t) &= \sum_{a\in\mathbb{Z}_N} (\nu_1 * \nu_2)(a) e_N(at) \\
&= \sum_{a\in\mathbb{Z}_N} \sum_{a_1+a_2=a} \nu_1(a_1)\nu_2(a_2) e_N(a_1 t) e_N(a_2 t) \\
&= \sum_{a_1\in\mathbb{Z}_N} \nu_1(a_1) e_N(a_1 t) \sum_{a_2\in\mathbb{Z}_N} \nu_2(a_2) e_N(a_2 t) = \widehat{\nu}_1(t)\widehat{\nu}_2(t). \qquad (3.1)
\end{aligned}$$

Now, (2) follows by induction. For (3) note that

$$\begin{aligned}
\frac{1}{N} \sum_{t\in\mathbb{Z}_N} \widehat{\nu}(t) &= \frac{1}{N} \sum_{t\in\mathbb{Z}_N} \sum_{a\in\mathbb{Z}_N} \nu(a) e_N(at) \\
&= \frac{1}{N} \sum_{a\in\mathbb{Z}_N} \nu(a) \sum_{t\in\mathbb{Z}_N} e_N(a) = \nu(0), \qquad (3.2)
\end{aligned}$$

where the last equality follows from the fact that for every $a \in \mathbb{Z}_N$, we have $\sum_{t\in\mathbb{Z}_N} e_N(at) = 0$ unless $a = 0$, in which case it is equal to N. □

We can now start with the proof of Lemma 3.4.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Proof of Lemma 3.4. Using parts (2) and (3) of Lemma 3.5, we have

$$\nu^{(n)}(0) = \frac{1}{N}\sum_{t\in\mathbb{Z}_N} \widehat{\nu}(t)^n,$$

Applying riangle inequality, we deduce

$$\nu^{(n)}(0) \le \frac{1}{N}\sum_{t\in\mathbb{Z}_N} |\widehat{\nu}(t)|^n.$$

Writing $\psi(t) = 1 - |\widehat{\nu}(t)|^2$ and using the inequality $|x| \le \exp\left(-\frac{1-x^2}{2}\right)$ that holds for all $x \in \mathbb{R}$, we obtain

$$\nu^{(n)}(0) \le \frac{1}{N}\sum_{t\in\mathbb{Z}_N} \exp\left(-\frac{n}{2}\psi(t)\right).$$

Set $f(t) = n\psi(t)$ and define $T(w) = \{t : f(t) \le w\}$. Note that since $f(0) = n\psi(0) = 0$, hence $0 \in T(w)$ for all $w \ge 0$.

By separating the sum into level sets, we obtain the following inequality:

$$\nu^{(n)}(0) \le \frac{1}{N}\int_0^\infty |T(w)| e^{-w/2} dw. \tag{3.3}$$

For an integer $k \ge 1$, and subsets $A_1, \dots, A_k \subseteq \mathbb{Z}_N$, we write

$$A_1 + \cdots + A_k := \{a_1 + \cdots + a_k : a_i \in A_i, \quad 1 \le i \le k\}.$$

We use the shorthand kA for $A + \cdots + A$, where k is the number of summands. The following lemma is proven in [[15], Proposition 3.5] for all finite fields. A simple verification shows that it applies verbatim to all finite cyclic groups. For reader's convenience, we will sketch the modification needed in the proof.

Lemma 3.6. *For any $w > 0$ and integer $k \ge 1$, we have*

$$kT(w) \subseteq T(k^2 w).$$

Proof. It suffices to show that for all $\beta_1, \dots, \beta_k \in \mathbb{Z}_N$, we have

$$\psi(\beta_1 + \cdots + \beta_k) \le k(\psi(\beta_1) + \cdots + \psi(\beta_k)).$$

This, in turn can be rewritten as:

$$1 - \sum_{a,b\in\mathbb{Z}_N} \mu(a)\mu(b)\cos\left(\frac{2\pi}{N}(a-b)(\beta_1 + \cdots + \beta_k)\right) \le k^2 - k\sum_{j=1}^{k}\sum_{a,b\in\mathbb{Z}_N} \mu(a)\mu(b)\cos\left(\frac{2\pi}{N}(a-b)\beta_j\right).$$

This follows from the trigonometric inequality proven in [[15], Proposition 3.1]. □

We will also need a lemma from additive combinatorics. Define the set of symmetries of a set $A \subseteq \mathbb{Z}_N$ by $\mathrm{Sym}A := \{h \in \mathbb{Z}_N : h + A = A\}$. Note that Sym$A$ is a subgroup of $\mathbb{Z}_N$ and if $0 \in A$ then $\mathrm{Sym}(A) \subseteq A$. The lemma follows by a simple inductive argument from [[22], Theorem 5.5].

Lemma 3.7 (Kneser's bound). *Let Z be an abelian group and $A_1, \dots, A_k \subseteq Z$ are finite subsets. Then we have*

$$|A_1 + \cdots + A_k| + (k-1)|\mathrm{Sym}(A_1 + \cdots + A_k)| \ge |A_1| + \cdots + |A_k|.$$

In particular, for any finite A we have

$$k|A| \le |kA| + (k-1)|\mathrm{Sym}(kA)|,$$

where $kA = A + \cdots + A$, with the sum containing k copies of A.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

We will now claim that if H is a subgroup of $\mathbb{Z}_N$ with $|H| \geq \frac{N}{r}$, then there exists $t \in H$ with $f(t) \geq n\beta$. To prove this note that

$$\frac{1}{|H|}\sum_{t\in H} f(t) = \frac{n}{|H|}\sum_{t\in H}(1-|\widehat{\nu}(t)|^2).$$

Expanding the definition of $\widehat{\nu}$ in $|\widehat{\nu}(t)|^2 = \widehat{\nu}(t)\cdot\overline{\widehat{\nu}(t)}$, and summing for $t \in H$ we obtain

$$\begin{aligned}\sum_{t\in H}|\widehat{\nu}(t)|^2 &= \sum_{t\in H}\sum_{\theta_1\in\mathbb{Z}_n}\nu(\theta_1)e_N(\theta_1 t)\sum_{\theta_2\in\mathbb{Z}_n}\nu(\theta_2)e_N(-\theta_2 t)\\ &= \sum_{t\in H}\sum_{\theta_1,\theta_2\in\mathbb{Z}_n}\nu(\theta_1)\nu(\theta_2)e_N((\theta_1-\theta_2)t) = |H|\cdot\sum_{\theta_1,\theta_2\in\mathbb{Z}_N}\nu(\theta_1)\nu(\theta_2)\mathbf{1}_{H^\perp}(\theta_1-\theta_2)\\ &= |H|\cdot\sum_{\theta_1\in\mathbb{Z}_N}\nu(\theta_1)\nu(\theta_1+H^\perp). \qquad (3.4)\end{aligned}$$

Here, $H^\perp$ denotes the dual of H, consisting of $x \in \mathbb{Z}_N$ such that $e_N(hx) = 1$ for all $h \in H$. Note that $H^\perp$ is a subgroup of $\mathbb{Z}_N$. If $\theta_1 \notin H^\perp$, then $0 \notin \theta_1 + H^\perp$ and hence $\nu(\theta_1 + H^\perp) \leq 1 - \nu(0) \leq 1 - \beta$. If $\theta_1 \in H^\perp$, then $\theta_1 + H^\perp = H^\perp$. Since $|H^\perp| \leq r$, we have $\nu(\theta_1 + H^\perp) \leq 1 - \beta$ in this case as well. This implies that $\sum_{t\in H}|\widehat{\nu}(t)|^2 \leq 1-\beta$. This shows that $\frac{1}{|H|}\sum_{t\in H} f(t) \geq n\beta$, implying that there exists $t \in H$ such that $f(t) \geq n\beta$.

Let us now suppose $w < n\beta$. Let k be the largest positive integer with $k^2 w < n\beta$. We claim that $|\mathrm{Sym}(kT(w))| \leq \frac{N}{r}$. In fact, if this is not the case, using Lemma 3.6 we have

$$kT(w) \subseteq T(k^2 w),$$

it follows that $T(k^2w)$ contains a subgroup H with more than N/r elements. We will then have

$$H \subseteq T(k^2 w) \subseteq T(n\beta)$$

which contradicts that claim proved above. It follows from Lemma 3.7 that for all $w < n\beta$, we have

$$|T(w)| \leq \frac{1}{k}|T(k^2 w)| + \frac{N}{r}.$$

By the choice of $k \geq 1$, we have

$$(2k)^2 w \geq (k+1)^2 w \geq n\beta$$

implying that $k \geq \sqrt{\frac{n\beta}{4w}}$. Putting all these together we obtain

$$|T(w)| \leq \sqrt{\frac{4w}{n\beta}}N + \frac{N}{r}.$$

Inserting the latter bound in the range $w < n\beta$ and the trivial bound $|T(w)| \leq N$ for $w > n\beta$ into (3.3), we arrive at

$$\begin{aligned}\nu^{(n)}(0) &\leq \frac{1}{2N}\int_0^{n\beta}\left(\sqrt{\frac{4w}{n\beta}}N + \frac{N}{r}\right)e^{-w/2}dw + \frac{1}{2N}\int_{n\beta}^{\infty} Ne^{-w/2}dw\\ &\leq \frac{C}{\sqrt{n\beta}}\int_0^{\infty}\sqrt{w}e^{-w/2}dw + \frac{1}{r} + \frac{1}{2}\int_{n\beta}^{\infty}e^{-w/2}dw\\ &\leq \frac{1}{r} + \frac{C'}{\sqrt{n\beta}} + e^{-n\beta/2} \qquad (3.5)\end{aligned}$$

This ends the proof of Lemma 3.4. □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Lemma 3.8. *Let ν be a probability measure on $\mathbb{Z}_N$ and $0 < \beta < 1/2$ such that $\beta \le \nu(0) \le 1-\beta$. Then for some constant C' and all $n \ge 1$, we have*

$$\nu^{(n)}(0) \le \frac{1}{2} + \frac{C'}{\sqrt{\beta n}} + e^{-n\beta/2}.$$

Proof. This is proven is similar to the proof of Lemma 3.4. As before we write

$$\nu^{(n)}(0) \le \frac{1}{N}\sum_{t\in\mathbb{Z}_N} |\,\widehat{\nu}(t)|^n \le \frac{1}{2N}\int_0^\infty |T(w)|e^{-w/2}dw.$$

We now claim that for all $w < n\beta$ we have

$$|T(w)| \le \sqrt{\frac{4w}{n\beta}}N + \frac{N}{2}.$$

To show this, for $w < n\beta$ denote by k the largest positive integer with $k^2 w < n\beta$. We claim that $|\mathrm{Sym}(T(w) + \cdots + T(w))| \le \frac{N}{2}$. Suppose that this is not the case. Recall that $T(w) = \{t : f(t) \le w\}$, where $f(t) = n\left(1 - |\widehat{\nu}(t)|^2\right)$. Since $\widehat{\nu}(0) = 1$, we have $f(0) = 0$. Since $w > 0$, we have $0 \in T(w)$. This implies that

$$\mathrm{Sym}(T(w) + \cdots + T(w)) \subseteq T(w) + \cdots + T(w) \subseteq T(k^2 w),$$

it follows that $T(k^2 w)$ contains a subgroup with more than $N/2$ elements, hence has to be equal to $\mathbb{Z}_N$, from which it follows that $T(n\beta) = \mathbb{Z}_N$. On the other hand, using the Plancherel formula we have

$$\frac{1}{N}\sum_{t\in\mathbb{Z}_N} |\widehat{\nu}(t)|^2 = \sum_{\theta_1\in\mathbb{Z}_N} \nu(\theta_1)^2 \le (1-\beta)^2 + \beta^2 \le 1-\beta,$$

where the second inequality follows from $(1-\beta) - (1-\beta)^2 - \beta^2 = \beta(1-2\beta) > 0$. This implies that $\frac{1}{N}\sum_{t\in\mathbb{Z}_N}(1 - |\widehat{\nu}(t)|^2) \ge \beta$. Hence, there exists $t \in \mathbb{Z}_N$ such that $f(t) \ge n\beta$. A similar argument as above finishes the proof. □

We will now combine Lemmas 3.1, 3.4, 3.8 to prove a non-concentration theorem for random walks on abelian groups with cyclic torsion component. Let $\Lambda := \Lambda_1 \times \Lambda_2$ where $\Lambda_1 \sim \mathbb{Z}^s$ and $\Lambda_2 \simeq \mathbb{Z}_N$ are free and torsion components of Λ. For $i = 1, 2$, denote the projection from Λ onto Λ_i by π_i, and for probability measure ν on Λ, we write $\nu_i := (\pi_i)_*\nu$ for the push-forward of ν under π_i.

Theorem 3.9 (Non-concentration for random walks on abelian groups). *Let Λ be a finitely generated abelian group with a cyclic torsion subgroup and ν a finitely supported probability measure on Λ. Let $0 < \beta < 1/2$ and $r \ge 1$ be a positive integer. Assume that*

1. *$\beta \le \nu(0) \le 1-\beta$.*
2. *$\nu(\Lambda^{\le r}) \le 1-\beta$, where $\Lambda^{\le r}$ is the subset of Λ consisting of elements of order at most r.*

Then for all $n \ge 1$, we have

$$\nu^{(n)}(0) \le \frac{1}{r} + \frac{C''}{\sqrt{n\beta}} + e^{-n\beta/4},$$

where C'' is an absolute constant. Moreover, only under assumption (1) above, we have

$$\nu^{(n)}(0) \le \frac{1}{2} + \frac{C''}{\sqrt{n\beta}} + e^{-n\beta/4}.$$

Proof. Clearly, we have

$$\nu^{(n)}(0) \le \min\left(\nu_1^{(n)}(0), \nu_2^{(n)}(0)\right).$$

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Moreover, the inequality $\beta \leq \nu_j(0)$ is satisfied for both $j = 1, 2$. We consider two cases: if $\nu_1(0) \leq 1 - \frac{\beta}{4}$, then it follows from Lemma 3.1 that

$$\nu^{(n)}(0) \leq \nu_1^{(n)}(0) \leq \frac{2C}{\sqrt{\beta n}}.$$

Hence, suppose that $\nu_1(0) > 1 - \frac{\beta}{4}$. We claim that in this case we must have $\nu_2(0) \leq 1 - \frac{\beta}{2}$. If this is not the case, then $\nu_2(0) \geq 1 - \frac{1}{2}\beta$ which contradicts assumption (2). We will now verify condition (2) of Lemma 3.4 by finding an upper bound on the measure (under ν_2) of the set of elements of order at most r in Λ_2:

$$\begin{aligned}\nu_2\{z \in \Lambda_2 : \mathrm{ord}_{\Lambda_2}(z) \leq r\} &= \nu\{z = (z_1, z_2) \in \Lambda : \mathrm{ord}_{\Lambda_2}(z_2) \leq r\} \\ &\leq \nu(\{z = (0, z_2) \in \Lambda : \mathrm{ord}(z) \leq r\}) + \nu(\{z = (z_1, z_2) \in \Lambda : z_1 \neq 0\}) \\ &\leq 1 - \beta + \frac{\beta}{4} < 1 - \frac{\beta}{2}. \end{aligned} \tag{3.6}$$

In particular, if H is a subgroup with $|H| \leq r$, then the order of every element of H is at most r, and hence $\nu_2(H) \leq 1 - \frac{\beta}{2}$. We can now apply Lemma 3.4 and Lemma 3.8 (with $\beta/2$ instead of β) to obtain the result. □

Corollary 3.10. *Let A be a matrix in $\mathrm{GL}_d(\mathbb{C})$ and $\beta > 0$. Assume that*

1. $\beta \leq \mathbf{m}_1(A) \leq 1 - \beta$.
2. $\mathbf{m}^{\leq r}(A) \leq (1 - \beta)$

Then for every $\eta > 0$ there exists $M := M(\beta, r, \eta)$ such that for all $n \geq M$, we have

$$\mathbf{m}_1(\mathsf{T}^n A) \leq \frac{1}{r} + \eta.$$

Moreover, only under assumption (1), for every $\eta > 0$ there exists $M' := M'(\beta, \eta)$ such that, for all $n \geq M'$ we have

$$\mathbf{m}_1(\mathsf{T}^n A) \leq \frac{1}{2} + \eta.$$

Proof. Denote by Λ the subgroup of $\mathbb{C}^*$ generated by the eigenvalues of A. Denote the subgroup of torsion elements in Λ by Λ_2 and let $\Lambda_1 \simeq \mathbb{Z}^s$ be a subgroup of Λ such that $\Lambda = \Lambda_1 \times \Lambda_2$. First suppose that conditions (1) and (2) hold. These guarantee that ξ_A satisfies (1) and (2) of Theorem 3.9. It follows that for all $n \geq 1$ we have

$$\xi_A^{(n)}(0) \leq \frac{1}{r} + \frac{C''}{\sqrt{n\beta}} + e^{-n\beta/4}.$$

Given $\eta > 0$, we can find $M = M(\beta, \eta)$ such that for all $n \geq M$ we have

$$\frac{C''}{\sqrt{n\beta}} + e^{-n\beta/4} < \eta.$$

This inequality together with the bound $\mathbf{m}_1(\mathsf{T}^n A) = \xi_A^{(n)}(1)$ establishes the claim. The second part of the statement (involving only assumption (1)) follows by a similar argument. □

4. Dynamics of the number of Jordan blocks under tensor powers

In this section, we will study the effect of amplification on matrices A with $\mathbf{m}_1(A)$ close to 1. If A is such a matrix, for $\rho(A - \mathrm{Id})$ to be away from zero, a definite proportion of its Jordan blocks have to be of size at least 2. We will show that under this condition, the proportion of the number of Jordan blocks to

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

the size of matrix tends to zero. Moreover, we will give an effective bound for the number of iterations required to reduce this ratio below any given positive ϵ.

We will denote by $J(\alpha, s)$ a Jordan block of size s with eigenvalue α. Let A be a $d \times d$ complex matrix. We denote by $\mathbf{j}(A)$ the number of Jordan blocks in the Jordan decomposition of A divided by d, hence $0 \leq \mathbf{j}(A) \leq 1$, with $\mathbf{j}(A) = 1$ iff A is diagonalizable. Define a sequence of matrices by setting

$$A_1 = A, \quad A_m = A_{m-1} \otimes A_{m-1}, \quad m \geq 1. \tag{4.1}$$

The main result of this section is the following theorem:

Theorem 4.1. *For every $\gamma > 0$ and every $\eta > 0$, there exists $N(\gamma, \eta)$ such that if $\mathbf{j}(A) \leq 1 - \gamma$ and $m > N(\gamma, \eta)$ then $\mathbf{j}(A_m) < \eta$, where A_m is defined by (4.1).*

The proof of this theorem will involve estimating certain trigonometric integrals. Before reformulating the problem, we will recall some elementary facts.

Lemma 4.2 ([3, 12], Lemma 5.7). *For $m, n \in \mathbb{N}$ and $\alpha, \beta \in \mathbb{C}$, we have*

$$J(\alpha, m) \otimes J(\beta, n) = \bigoplus_{i=1}^{\min(m,n)} J(\alpha\beta, m + n + 1 - 2i).$$

Remark 4.3. *It follows from this lemma that the number of Jordan blocks of a given size in tensor powers of A only depends on the size of Jordan blocks in A and not on the corresponding eigenvalues. We will use this simple fact later.*

In order to study the asymptotic behavior of the number of Jordan blocks in tensor powers of A, it will be convenient to set up some algebraic framework. Let us denote by $\mathcal{A}$ the set of all $n \times n$ matrices in the Jordan normal form with eigenvalue 1 on the diagonal, where $n \geq 1$ varies over the set of all natural numbers. Note that if $A \in \mathcal{A}$, then $A \otimes A \in \mathcal{A}$. We will denote by $\mathcal{E}$ the set of all formal linear combinations $\sum_{n \geq 1} c_n \delta_n$, where $c_n \geq 0$ are integers and $c_n = 0$ for all but finitely many values of n. We equip $\mathcal{E}$ with a binary operation defined by:

$$\delta_m * \delta_n = \sum_{i=1}^{\min(m,n)} \delta_{m+n+1-2i}$$

and extended linearly to $\mathcal{T}$. Finally, for $n \geq 1$, consider the Laurent polynomial

$$T_n(x) = \sum_{i=1}^{n} x^{n-2i+1} = x^{n-1} + x^{n-3} + \ldots + x^{-(n-3)} + x^{-(n-1)},$$

and denote by $\mathcal{T}$ the set of all (finite) integer linear combinations of $\{T_n(x)\}_{n \geq 1}$. Note that since T_n have different degrees, they do form a basis for the $\mathbb{Z}$-module $\mathcal{T}$.

Now we will construct natural maps between these objects that will allow us to encode the number and size of Jordan blocks in tensor powers of a matrix using polynomials $T_n(x)$. First, define the map $\Delta : \mathcal{A} \to \mathcal{E}$ as follows. Let $A \in \mathcal{A}$ be a matrix with c_i blocks of size i for $i \geq 1$. Then define

$$\Delta(A) = \sum_{n \geq 1} c_n \delta_n.$$

Note that Δ is a bijection. We now define $\Theta : \mathcal{E} \to \mathcal{T}$ by

$$\Theta\left(\sum_{n \geq 1} c_n \delta_n\right) = \sum_{n \geq 1} c_n T_n(x).$$

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Lemma 4.4. *The following hold:*

1. *For all $A_1, A_2 \in \mathcal{A}$, we have $\Delta(A_1 \otimes A_2) = \Delta(A_1) * \Delta(A_2)$.*
2. *For all $x_1, x_2 \in \mathcal{E}$, we have $\Theta(x_1 * x_2) = \Theta(x_1)\Theta(x_2)$.*

Proof. For (1), note that when A_1 consists of one block of size m and A_2 is a block of size n, this is a restatement of Lemma 4.2. In this case, we have $\Delta(A_1) = \delta_m$ and $\Delta(A_2) = \delta_n$ and $\Delta(A_1 \otimes A_2)$ is precisely the expression defined by $\delta_m * \delta_n$. It follows immediately from the definition of tensor product of matrices that the equality extends to all linear combinations with nonnegative integer coefficients. This establishes (1).

In order to prove (2), we will show that For $m, n \in \mathbb{N}$, the following identity holds:

$$T_m(x)T_n(x) = \sum_{i=1}^{\min(m,n)} T_{m+n+1-2i}(x).$$

Without loss of generality, assume that $m \leq n$. We will proceed by calculating the coefficient of x^r for $r \in \mathbb{Z}$ on both sides. Note that x^r appears on either the right-hand side or the left-hand side if and only if $r = m + n - 2j$ for some $1 \leq j \leq m + n - 1$. Since the coefficients of x^j and x^{-j} are equal, it suffices to consider the coefficient of x^r for nonnegative values of r, which correspond to $0 \leq j \leq \frac{m+n}{2}$. Fix j in this range. It follows from the definition that x^{m+n-2j} appears in $T_{m+n+1-2k}$ if and only if $m + n - 2k \geq m + n - 2j$, or, equivalently if $k \leq j$. Since we have $1 \leq k \leq m$, the term x^{m+n-2j} appears exactly $\min(j, m)$ times on the right-hand side. We now show that the coefficient of x^{m+n-2j} on the left-hand side is the same. Note that the coefficient of the term x^r with $r = m + n - 2j$ in $T_m T_n$ is equal to the number of pairs (j_1, j_2) such that x^{m+1-2j_1} appears in T_m and x^{n+1-2j_2} appears in T_n where $(m + 1 - 2j_1) + (n + 1 - 2j_2) = m + n - 2j$. These conditions can be reformulated as below:

$$j_1 + j_2 = j + 1 \qquad 1 \leq j_1 \leq m, 1 \leq j_2 \leq n. \tag{4.2}$$

Let us distinguish two cases: first suppose that $j \leq m$. In this case, we choose $1 \leq j_1 \leq j$ and any such choice determines $j_2 = j + 1 - j_1$ uniquely. Hence, the number of solutions to (4.2) is j. When $j > m$, then j_1 is allowed to vary in the range $1 \leq j_1 \leq m$, and since $j \leq \frac{m+n}{2}$, $j_2 := j + 1 - j_1$ will automatically satisfy the inequality $1 \leq j_2 \leq n$. In conclusion, the coefficient of x^{m+n-2j} on the left-hand side equals $\min(j, m)$ as well. This proves the claim. It thus follows that $\Theta(x_1 * x_2) = \Theta(x_1)\Theta(x_2)$ holds for $x_1 = \delta_m$ and $x_2 = \delta_n$. Since Θ is extended to $\mathcal{E}$ by linearity, the general case follows immediately. □

Corollary 4.5. *Let A be a $d \times d$ invertible complex matrix. Let $a_n^{(k)}$ be the multiplicity of Jordan blocks of size n in the Jordan decomposition of A_k:*

$$\left(\sum_{n\geq 1} a_n^{(1)} T_n(x)\right)^{2^{k-1}} = \sum_{n\geq 1} a_n^{(k)} T_n(x)$$

Proof. Using Remark 4.3, we can assume that all eigenvalues are equal to 1, or $A \in \mathcal{A}$. It is clear that $\Delta(A) = \sum_{n\geq 1} a_n^{(1)} \delta_n$. Part (1) of Lemma 4.4 implies that

$$\Delta(A_m) = \Delta(A_{m-1} \otimes A_{m-1}) = \Delta(A_{m-1}) * \Delta(A_{m-1}).$$

Since $\Delta(A_m) = \sum_{n\geq 1} a_n^{(m)} \delta_n$, applying Θ to the previous equation and using part (2) of Lemma 4.4 give

$$\sum_{n\geq 1} a_n^{(m)} T_n(x) = \left(\sum_{n\geq 1} a_n^{(m-1)} T_n(x)\right)^2.$$

The claim follows by induction on m. □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

It will be more convenient to work with a trigonometric generating function. This is carried out in the next lemma.

Corollary 4.6. *With the same notation as in Corollary 4.5, set*

$$P_k(\theta) = \frac{1}{d}\sum_{n\geq 1} a_n^{(k)} \frac{\sin(n\theta)}{\sin(\theta)}.$$

For all $k \geq 1$, we have

$$P_1(\theta)^{2^k} = P_k(\theta)$$

Proof. Substituting $x = e^{i\theta}$ into $T_n(x)$ yields

$$T_n(e^{i\theta}) = \sum_{i=1}^{n} e^{i(n-2i+1)\theta} = \frac{e^{in\theta} - e^{-in\theta}}{e^{i\theta} - e^{-i\theta}} = \frac{\sin(n\theta)}{\sin(\theta)}.$$

By applying Corollary 4.5, we obtain

$$\left(\sum_{n\geq 1} a_n^{(1)} \frac{\sin(n\theta)}{\sin(\theta)}\right)^{2^k} = \sum_{n\geq 1} a_n^{(k)} \frac{\sin(n\theta)}{\sin(\theta)}.$$

□

Lemma 4.7. *Let $0 \leq \epsilon \leq 2$ and $2 \leq n \in \mathbb{N}$. For any real number θ such that $|\cos(\theta)| \leq 1 - \frac{\epsilon}{2}$, we have*

$$\left|\frac{\sin(n\theta)}{\sin(\theta)}\right| \leq n - \epsilon.$$

In particular, $|\frac{\sin(n\theta)}{\sin(\theta)}| \leq n$ holds for all $\theta \in \mathbb{R}$.

Proof. We will proceed by induction on n. For $n = 2$, the required inequality is obvious. Assume that it also holds for n. One can write:

$$\left|\frac{\sin((n+1)\theta)}{\sin(\theta)}\right| = \left|\frac{\sin(n\theta)\cos(\theta) + \sin(\theta)\cos(n\theta)}{\sin(\theta)}\right| \leq \left|\frac{\sin(n\theta)}{\sin(\theta)}\right| \cdot |\cos(\theta)| + |\cos(n\theta)| \leq n - \epsilon + 1$$

Thus, the required inequality holds for $n+1$ as well and we are done. □

Corollary 4.8. *For all $\theta \in \mathbb{R}$, we have $|P_1(\theta)| \leq 1$.*

Proof. This follows immediately from Lemma 4.7 and the equality $\sum_{n\geq 1} n a_n^{(1)} = d$. □

For a measurable subset $B \subseteq \mathbb{R}$, we denote by $\mu(B)$ is the Lebesgue measure of B. We will also denote the number of Jordan blocks of size 1 in A by $\mathbf{j}_1(A)$.

Lemma 4.9. *Suppose that $A \in \mathrm{GL}_d(\mathbb{C})$ is in the Jordan normal form. For $\epsilon > 0$, set*

$$B_\epsilon := \left\{\theta \in [0, 2\pi] : |P_1(\theta)| \leq 1 - (\mathbf{j}(A) - \mathbf{j}_1(A))\epsilon\right\}.$$

Then

$$\mu([0, 2\pi] \setminus B_\epsilon) \leq 8\sqrt{\epsilon}.$$

Proof. If all Jordan blocks are of size 1, then $\mathbf{j}_1(A) = \mathbf{j}(A)$ and the claim follow Corollary 4.8. More generally, suppose $\cos(\theta) \leq 1 - \frac{\epsilon}{2}$. Then it follows from Lemma 4.7 that

$$1 - |P_1(\theta)| = \frac{1}{d}\sum_{m\geq 2}\left(m - \left|\frac{\sin(m\theta)}{\sin(\theta)}\right|\right) a_m^{(1)} \geq \frac{1}{d}\sum_{m\geq 2} \epsilon a_m^{(1)} = \epsilon(\mathbf{j}(A) - \mathbf{j}_1(A))$$

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

This implies that $\theta \in B_\epsilon$. Hence,

$$\mu([0, 2\pi] \setminus B_\epsilon) \leq 4 \cos^{-1}(1 - \epsilon/2) \leq 8\sqrt{\epsilon},$$

where one can easily verify the last inequality for all $\epsilon \in (0, 1)$. □

Lemma 4.10. *Suppose $A \in \mathrm{GL}_d(\mathbb{C})$ is not unipotent, that is, $\mathbf{j}(A) < 1$. Then we have $\mathbf{j}_1(A \otimes A) \leq \mathbf{j}(A)^2$.*

Proof. First, notice that $J(\alpha, s) \bigotimes J(\beta, t)$ generates a Jordan block of size 1 if and only if the equation $s + t + 1 - 2i = 1$ holds for some $1 \leq i \leq \min(s, t)$. Equivalently $s + t = 2i$ for $1 \leq i \leq \min(s, t)$. This equation has a solution if and only if $s = t$. Therefore, we have

$$\mathbf{j}_1(A \otimes A) = \frac{\sum_{n \geq 1} (a_n^{(1)})^2}{d^2} \leq \left(\frac{\sum_{n \geq 1} a_n^{(1)}}{d} \right)^2 = \mathbf{j}(A)^2.$$ □

Lemma 4.11. *For $a, b \in \mathbb{R}$, define $I_n(a, b) = \int_a^b \frac{\sin(n\theta)}{\sin(\theta)} d\theta$. Then for all $n \in \mathbb{Z}$ we have*

$$(n + 1)\big(I_{n+2}(a, b) - I_n(a, b)\big) = 2\big[\sin((n + 1)b) - \sin((n + 1)a)\big].$$

Proof. As a, b are fixed during this proof, we write I_n instead of $I_n(a, b)$. First note that

$$I_{n+2} = \int_a^b \frac{\sin((n + 2)\theta)}{\sin(\theta)} d\theta = \int_a^b \frac{\sin(n\theta)\cos(2\theta)}{\sin(\theta)} d\theta + \int_a^b \frac{\sin(2\theta)\cos(n\theta)}{\sin(\theta)} d\theta$$

Using $\cos(2\theta) = \cos^2(\theta) - \sin^2(\theta) = 1 - 2\sin^2(\theta)$, we can write

$$\begin{aligned} I_{n+2} &= \int_a^b \frac{\sin(n\theta)(1 - 2\sin^2(\theta))}{\sin(\theta)} d\theta + 2\int_a^b \cos(\theta)\cos(n\theta) d\theta \\ &= \int_a^b \frac{\sin(n\theta)}{\sin(\theta)} d\theta - 2\int_a^b \sin(\theta)\sin(n\theta) d\theta + 2\int_a^b \cos(\theta)\cos(n\theta) d\theta \\ &= I_n + 2\int_a^b (\cos(n\theta)\cos(\theta) - \sin(n\theta)\sin(\theta)) d\theta \\ &= I_n + 2\int_a^b \cos((n + 1)\theta) d\theta = I_n + \frac{2}{n + 1}(\sin((n + 1)b) - \sin((n + 1)a). \end{aligned}$$ □

Corollary 4.12.

1. *For all odd integers n, we have*

$$I_n(0, 2\pi) = 2\pi, \quad I_n(\frac{\pi}{2}, \frac{3\pi}{2}) = \pi.$$

2. *For all even integers n, we have*

$$I_n(0, 2\pi) = 0, \quad I_n(\frac{\pi}{2}, \frac{3\pi}{2}) \geq 3.$$

Proof. A direct computation shows that $I_2(0, 2\pi) = 0$ and $I_1(0, 2\pi) = 2\pi$. Repeated application of Lemma 4.11 extends this to all integers n. In a similar fashion, checking that $I_1(\pi/2, 3\pi/2) = \pi$ together with $\sin((n + 1)\frac{\pi}{2}) = \sin(3(n + 1)\frac{\pi}{2}) = 0$ implies the claim for all odd values of n. The last inequality is easy to check for $n = 2, 4$. For $n \overset{4}{\equiv} 0$, we have

$$I_{n+2} = I_n - \frac{4}{n + 1} = I_{n-2} + \frac{4}{n - 1} - \frac{4}{n + 1} > I_{n-2} \geq 3$$

and for $n \overset{4}{\equiv} 2$ we can write

$$I_{n+2} = I_n + \frac{4}{n + 1} > I_{n-2} \geq 3.$$ □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Corollary 4.13. *Let $A \in \mathrm{GL}_d(\mathbb{C})$ and $P_k(\theta)$ be defined as above. Then we have*

$$\mathbf{j}(A_k) \leq \frac{1}{3}\int_0^{2\pi} P_1(\theta)^{2^k}\, d\theta.$$

Proof. Using Corollary 4.6 and Corollary 4.12, we can write

$$\begin{aligned}\int_0^{2\pi} P_1(\theta)^{2^k} d\theta &\geq \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} P_1(\theta)^{2^k} d\theta = \sum_{n\geq 1} \frac{a_n^{(k)}}{d^{2^k}} \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} \frac{\sin(n\theta)}{\sin(\theta)} d\theta \\ &\geq 3\sum_{n\geq 1} \frac{a_{2n}^{(k)}}{d^{2^k}} + 2\pi \sum_{n\geq 1} \frac{a_{2n-1}^{(k)}}{d^{2^k}} \geq 3\mathbf{j}(A_k).\end{aligned}$$

□

Proof of Theorem 4.1. Let $A \in \mathrm{GL}_d(\mathbb{C})$ be such that $\mathbf{j}(A) \leq \frac{1}{t}$, where $t = (1-\gamma)^{-1} > 1$. Let $\tau < \frac{1}{2}(\gamma/(1-\gamma))^2$. We will find a function $N_0(\gamma)$ such that for all $m \geq N_0(\gamma)$ we have $\mathbf{j}(A_m) \leq \frac{1}{t+\tau}$. By repeating this process, we see that for all $\ell \geq 1$ and all $m \geq \ell N_0(\gamma)$ we have $\mathbf{j}(A_m) \leq \frac{1}{t+\ell\tau}$. Let k be defined by $k = \lceil (\eta\tau)^{-1} \rceil + 1$ so that $k\tau > \eta^{-1}$. It is clear that

$$N(\gamma, \eta) = kN_0(\gamma)$$

will satisfy the required property.

If we have $\mathbf{j}(A \otimes A) \leq \frac{1}{t+\tau}$ we set $m = 2$, and we are done. Note that Proposition 5.8. of [3], we have $\mathbf{j}(B \otimes B) \leq \mathbf{j}(B)$ for any matrix B. Since $A_{m+1} = A_m \otimes A_m$, it follows that if we once the inequality holds for $m = 2$ then the same inequality will continue to hold for all $m \geq 2$. Set let us assume that $\mathbf{j}(A \otimes A) > \frac{1}{t+\tau}$. Then, we have

$$\begin{aligned}\int_0^{2\pi} P_1(\theta)^{2^k} d\theta &= \int_{B_\epsilon} |P_1(\theta)|^{2^k} d\theta + \int_{[0,2\pi]\setminus B_\epsilon} |P_1(\theta)|^{2^k} d\theta \\ &\leq \int_{B_\epsilon} (1 - \epsilon(\mathbf{j}(A) - \mathbf{j}_1(A)))^{2^k} d\theta + \int_{[0,2\pi]\setminus B_\epsilon} d\theta \\ &\leq 2\pi(1 - \epsilon(\mathbf{j}(A) - \mathbf{j}_1(A)))^{2^k} + \mu([0,2\pi] \setminus B_\epsilon) \\ &\leq 2\pi\left(1 - \frac{1}{t+\tau}\epsilon + \frac{1}{t^2}\epsilon\right)^{2^k} + 8\sqrt{\epsilon}\end{aligned}$$

It follows from the choice of τ that $\frac{1}{t+\tau} > \frac{2}{t^2}$. This implies that

$$\int_0^{2\pi} P_1(\theta)^{2^k} d\theta \leq 2\pi\left(1 - \frac{\epsilon}{t^2}\right)^{2^k} + 8\sqrt{\epsilon}.$$

Set $\epsilon = \frac{1}{2^8(t+\tau)^2} < \frac{1}{2t^2}$ so that the second term is bounded by $\frac{1}{2(t+\tau)}$. Now, let $N_0(\gamma)$ be the smallest positive integer m such that

$$2\pi\left(1 - \frac{\epsilon}{t^2}\right)^{2^m} < \frac{1}{2(t+\tau)}.$$

It is clear that for this value of m, we have

$$\int_0^{2\pi} P_1(\theta)^{2^m} d\theta \leq \frac{1}{t+\tau}.$$

The claim will now follow from Corollary 4.13. □

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

5. Proof of Theorem A

In this section, we will prove parts (1) and (2) of Theorem A. The proof crucially depends on the inequality

$$\rho(A, \mathrm{Id}) \geq \max\,(1 - \mathbf{m}_1(A), 1 - \mathbf{j}(A)).$$

from Lemma 2.1. Let G be a torsion-free group and S a finite subset of G with $e \notin S$. We will show that for every $\epsilon > 0$ and $\delta > 0$ an $(S, \delta, 1-\epsilon)$-map into $\mathrm{GL}_D(\mathbb{C})$ exists. Let $r = \lfloor 2/\epsilon \rfloor + 1$ and set $\overline{S} = \{g^n : g \in S, 1 \leq n \leq r!\}$. By Lemma 2.4, there exists an $(\overline{S}, \delta_0, 0.23)$-map ϕ_0 such that

$$\mathbf{m}_1(\phi_0(g)) \geq 0.01 \tag{5.1}$$

for all $g \in \overline{S}$. Here, δ_0 is a small quantity whose values will be determined later. We will find N such that for $n > N$, the tensor power $\mathsf{T}^{2^n}\phi_0$ is an $(S, \delta, 1-\epsilon)$-map. Fix some $g \in S$. We will consider two different cases.

Case (1): Suppose that $\mathbf{j}(\phi_0(g^{r!})) < 0.99$. Then it follows from Lemma 2.5 and Theorem 4.1 that for $m = N(0.01, \epsilon/2)$ we have $\mathbf{j}(\mathsf{T}^{2^m}\phi_0(g^{r!})) \leq \epsilon$. This implies that

$$\rho(\mathsf{T}^{2^m}\phi_0(g^{r!}), \mathrm{Id}) \geq 1 - \epsilon/2$$

On the other hand, using Lemma 2.5, we have

$$\rho(\mathsf{T}^{2^m}\phi_0(g^{r!}), \mathsf{T}^{2^m}\phi(g)^{r!}) \leq 2^m \rho(\phi_0(g^{r!}), \phi(g)^{r!}) \leq 2^m r!\delta_0 < \epsilon/2$$

as soon as $\delta_0 < \epsilon/2^{m+1}r!$. From here, we have by the triangle inequality that

$$\rho(\mathsf{T}^{2^m}\phi_0(g)^{r!}, \mathrm{Id}) \geq 1 - \epsilon.$$

Note that if B is any matrix and $m \geq 1$, then $\ker(B - I) \subseteq \ker(B^m - I)$. In other words, we have $\rho(B, I) \geq \rho(B^m, I)$. This implies that $\rho(\mathsf{T}^{2^m}\phi_0(g), \mathrm{Id}) \geq 1 - \epsilon$.

Case (2): Suppose that $\mathbf{j}(\phi_0(g^{r!})) \geq 0.99$. The proportion of blocks corresponding to eigenvalue 1 is $\mathbf{j}_1(\phi_0(g^{r!}))$, and the proportion of other blocks is at most $1 - \xi_{\phi_0(g^{r!})}(1)$. This implies that

$$\mathbf{j}_1(\phi_0(g^{r!})) + 1 - \xi_{\phi_0(g^{r!})}(1) \geq 0.99.$$

Since $\mathbf{j}_1(\phi_0(g^{r!})) = 1 - \rho(\phi_0(g^{r!}), \mathrm{Id}) \leq 1 - 0.23 = 0.77$, we obtain

$$\rho(\phi_0(g^{r!}), \mathrm{Id}) \geq 1 - \mathbf{m}_1(\phi_0(g^{r!}) = 1 - \xi_{\phi_0(g^{r!})}(1) \geq 0.22.$$

Also note that

$$\rho(\phi_0(g)^{r!}, \phi_0(g^{r!})) \leq r!\delta_0.$$

It thus follows that

$$\rho(\phi_0(g)^{r!}, \mathrm{Id}) \geq 0.22 - r!\delta_0 \geq 0.21$$

as long as $\delta_0 < \frac{1}{100\,r!}$. If D denotes the size of the matrix $\phi_0(g)^{r!}$, then we know that $\phi_0(g)^{r!}$ has at least $0.99D$ Jordan blocks. If k denotes the number of blocks corresponding to the eigenvalue 1, then noting that each such block contributes a one-dimensional subspace to $\ker(\phi_0(g)^{r!} - I)$, we deduce that $k \leq 0.21D$. Note that by the assumption $\mathbf{j}(\phi_0(g^{r!})) \geq 0.99$, that is, $\phi_0(g^{r!})$ has at least $0.99D$ Jordan blocks. This means that the total number of eigenvalues (with multiplicity) coming from blocks of size at least 2 is at most $0.01D$. Hence, the multiplicity of 1 as an eigenvalue of $\phi_0(g^{r!})$ is at most $0.23D$.

Note that if $(\lambda_i)_{1 \leq i \leq d}$ are eigenvalues of $\rho(g)$, then $(\lambda_i^{r!})$ are eigenvalues of $\rho(g)^{r!}$. If $\lambda_i^k = 1$ for some $1 \leq k \leq r$, then $\lambda_i^{r!} = 1$. This implies that

$$\mathbf{m}^{\leq r}(\phi_0(g)) \leq \mathbf{m}_1(\phi_0(g)^{r!}) = \xi_{\phi_0(g)^{r!}}(1) \leq 1 - \beta. \tag{5.2}$$

for $\beta = 0.23$. Applying Lemma 3.10 it follows that for $m > M(\beta, r, 1/r)$, we have

$$\mathbf{m}_1(\mathsf{T}^m\phi_0(g)) \leq \frac{2}{r} \leq \epsilon.$$

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

It follows that $\rho(\mathsf{T}^m\phi_0(g)), \mathrm{Id}) \geq 1-\epsilon$. In conclusion, for $m > \max(M(\beta, r, 1/r), N(0.01, \epsilon))$, we have

$$\rho\left(\mathsf{T}^m\phi_0(g)\right), \mathrm{Id}) \geq 1-\epsilon.$$

for all $g \in S$. Note, however, that

$$\rho\left(\mathsf{T}^m\phi_0(g)\mathsf{T}^m\phi_0(h), \mathsf{T}^m\phi_0(gh)\right) \leq 2^m\delta_0.$$

Hence, we need to choose $\delta_0 < \min\left(\frac{1}{100\,r!}, \frac{\delta}{2^N}, \frac{\epsilon}{2^{m+1}r!}\right)$ with $N = \max(M(\beta, r, 1/r), N(0.01, \epsilon))$ for the desired inequality to hold. The proof of (2) is similar and somewhat simpler. This time, we work directly with S (and not $\overline{S}$) and apply part (2) of Corollary 3.10.

Remark 5.1. *One can deduce from Theorem A the more general version in which the field of complex numbers is replaced by an arbitrary field of characteristic zero F. In order to see this, suppose that G is κ-linear sofic over F. This implies that for every finite set $S \subseteq G$ and every $\delta > 0$ and every $0 \leq \kappa' < \kappa$, there exists $d \geq 1$ and a map $\phi : S \to \mathrm{GL}_d(F)$ that satisfies properties (AH) and (D) of Definition 1.1. Since S is finite, one can replace F by a finitely generated subfield F' of F (depending on S). However, every such field is isomorphic to a subfield of $\mathbb{C}$. This implies that the arguments given above show that one can amplify ϕ. Now, note that all the amplifications are constructed via the functorial operations describe in 2.1. This implies that the image remains in $\mathrm{GL}_m(F)$ for some $m \geq 1$, from which the claim follows.*

Remark 5.2. *The part of the proof that is based on Lemma 4.2 does not work over fields of positive characteristic. In fact, the entire section 4 uses heavily the special form of this formula. It would be interesting to see if the method can be generalized to fields of positive characteristic.*

6. Stability and the proof of Theorems B and C

In this section, we will prove Theorem B. Along the way, we will also address the more general question of determining $\kappa(G)$ when G is an arbitrary finite group. As a byproduct, we will show that the bound $\kappa(G) \geq 1/2$ cannot be improved for finite groups. This will be carried out through computation of $\kappa(\mathbb{Z}_p^n)$, from which it will follow that as $n \to \infty$

$$\kappa\left(\mathbb{Z}_p^n\right) \to 1 - \frac{1}{p}.$$

The special case of $p = 2$ will then prove the claim. One ingredient of the proof is the notion of *stability* for linear sofic representations. Studying stability for different modes of metric approximation has been an active area of research in the last decade. Stability of finite groups for sofic approximation was proved by Glebsky and Rivera [10]. Arzhantseva and Păunescu [2] showed that abelian groups are stable for sofic approximation. This result was generalized by Becker, Lubotzky, and Thom [5] who established a criterion in terms of invariant random subgroups for (sofic) stability in the class of amenable groups. For other related results, see for instance [2, 6, 5, 4] and references therein. Some progress toward proving the stability of $\mathbb{Z}^2$ in linear sofic approximation has been made in [7]. Our first theorem establishes the stability of finite groups in the normalized rank metric. Before stating and proving this result, we will need a simple fact from linear algebra.

Lemma 6.1. *Suppose that $W_1, \ldots, W_i$ are subspaces of $\mathbb{C}^d$ with $\dim(W_r) \geq d(1-\epsilon)$, for $1 \leq i \leq r$. Then, we have $\dim(\cap_{i=1}^r W_i) \geq d(1-r\epsilon)$.*

Proof. We will proceed by induction on r. For $r = 1$ there is nothing to prove. Assume that the claim is shown for $r-1$. Then, using the induction hypothesis, one can write

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

$$\begin{aligned}\dim(\cap_{i=1}^{r} W_i) &= \dim(\cap_{i=1}^{r-1} W_i) + \dim(W_r) - \dim(\cap_{i=1}^{k-1} W_i + W_r)\\ &\geq d(1-(r-1)\epsilon) + d(1-\epsilon) - d\\ &= d(1-r\epsilon)\end{aligned}$$

□

Proposition 6.2. *Let G be a finite group, $\epsilon > 0$ and $\varphi : G \to \mathrm{GL}_d(\mathbb{C})$ is such that for all $g, h \in G$ we have*

$$\rho(\varphi(g)\varphi(h) - \varphi(gh)) < \epsilon.$$

Then there exists a representation $\psi : G \to \mathrm{GL}_d(\mathbb{C})$ such that for every $g \in G$ we have

$$\rho(\varphi(g), \psi(g)) < |G|^2\epsilon.$$

Proof. For $g, h \in G$, consider the subspace defined by

$$W_{g,h} = \ker(\varphi(g)\varphi(h) - \varphi(gh))$$

and set $W = \cap_{g,h\in G} W_{g,h}$. We claim that W is a G-invariant subspace of $\mathbb{C}^d$. Assume that w_1 is an arbitrary element of W. It suffices to prove that for any $k \in G$, $\varphi(k)w_1$ is an element of W as well. Since $w_1 \in W$, we can write

$$\begin{aligned}\varphi(g)\varphi(h)\big(\varphi(k)w_1\big) &= \varphi(g)\big(\varphi(h)\varphi(k)w_1\big)\\ &= \varphi(g)\varphi(hk)w_1 = \varphi(ghk)w_1\\ &= \varphi(gh)(\varphi(k)w_1)\end{aligned}$$

This implies that $\varphi(k)w_1 \in W_{g,h}$, proving the claim. In summary, $W \leq \mathbb{C}^d$ is a G-invariant subspace with the property that the restriction of $\psi(g)$ to W is a representation of G. Let $W^\perp$ be a subspace complement of W. For $g \in G$, define $\psi(g) \in \mathrm{GL}_d(\mathbb{C})$ to be the linear transformation that acts on W via φ and on $W^\perp$ by identity. It is clear that ψ defined in this way is a G-representations. Finally, for every $g \in G$ we have

$$\mathrm{rank}(\psi(g) - \varphi(g)) \leq \dim(W^\perp) = d - \dim(W) \leq d|G|^2\epsilon.$$

This finishes the proof. □

Remark 6.3. *It is noteworthy that our proof establishes stability with a linear estimate. However, the constant depends on $|G|$. It would be interesting to see if this dependency can be relaxed for certain families of groups.*

We will start by providing a simple description of irreducible representations of the group $G = \mathbb{Z}_p^n$. We start by setting some notation. Recall that $\mathrm{e}_p : \mathbb{Z}_p \to \mathbb{C}^*$ denotes the character $\mathrm{e}_p(x) = \exp(2\pi ix/p)$. Also, for $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$, we write $x \cdot y = \sum_{i=1}^n x_i y_i$. For each $a \in \mathbb{Z}_p^n$, define $\phi_a : \mathbb{Z}_p^n \to \mathbb{C}^*$ by $\phi_a(x) = \mathrm{e}_p(a \cdot x)$. It is a well known [14] fact that ϕ_a, as $a \in \mathbb{Z}_p^n$ constitute all irreducible representations of $\mathbb{Z}_p^n$.

Proposition 6.4. *For $n \geq 2$, we have*

$$\kappa\big(\mathbb{Z}_p^n\big) = \frac{p^n - p^{n-1}}{p^n - 1}.$$

Proof. Let

$$\phi := \bigoplus_{a\neq 0} \phi_a$$

denote the direct sum of all ϕ_a other than the trivial representation ϕ_0. One can regard $\phi(x)$ as a diagonal matrix of size $p^n - 1$ with diagonal entries $\phi_a(x)$ for nonzero $a \in \mathbb{Z}_p^n$. We claim that for every $x \neq 0$,

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

the set of $\{a \in \mathbb{Z}_p^n \setminus \{0\} : \phi_a(x) = 1\}$ has cardinality p^{n-1}. In fact, the condition $\phi_a(x) = 1$ corresponds to the equation $\sum_{i=1}^n a_i x_i = 0$ for a which has exactly $p^{n-1} - 1$ nonzero solutions. Hence, $\operatorname{rank}\phi(x) = p^n - p^{n-1}$, from which it follows that

$$\rho(\mathrm{Id}, \phi(x)) = \frac{p^n - p^{n-1}}{p^n - 1}.$$

To prove the reverse inequality, we first suppose ψ is a d-dimensional representation of G. Decompose ψ into a direct sum of irreducible representations ϕ_a and denote the multiplicity of ϕ_a by c_a:

$$\phi = \bigoplus_a c_a \phi_a.$$

Set

$$\beta := \min_{g \in G} \frac{1}{d} \operatorname{rank}(\psi(g) - \mathrm{Id}),$$

and write $B(x) = \{a \in \mathbb{Z}_p^n : \phi_a(x) \neq 1\}$. This implies that for every nonzero $x \in \mathbb{Z}_p^n$, we have

$$\sum_{a \in B(x)} c_a \geq \beta d \quad \Rightarrow \quad \sum_{x \neq 0} \sum_{a \in B(x)} c_a \geq \beta d (p^n - 1). \tag{6.1}$$

Without loss of generality, we can assume that $c_0 = 0$, since by removing the trivial representation the value of β can only increase. Note also that for every $a \neq 0$, there are exactly $p^n - p^{n-1}$ elements $x \in \mathbb{Z}_p^n$ with $a \in B(x)$. This implies that

$$\sum_{x \neq 0} \sum_{a \in B(x)} c_a = \left(p^n - p^{n-1}\right) \sum_{a \neq 0} c_a = d\left(p^n - p^{n-1}\right),$$

This together with (6.1) implies that $\beta \leq \frac{p^n - p^{n-1}}{p^n - 1}$.

Now, to finish the proof assume that $\beta := \kappa(\mathbb{Z}_p^n) > \frac{p^n - p^{n-1}}{p^n - 1}$. Choose $\epsilon > 0$ such that $p^{2n}\epsilon < \beta - \frac{p^n - p^{n-1}}{p^n - 1}$. Let $\varphi : \mathbb{Z}_p^n \to \mathrm{GL}_d(\mathbb{C})$ be such that

$$\rho(\varphi(x)\varphi(y) - \varphi(x + y)) < \epsilon.$$

holds for all $x, y \in \mathbb{Z}_p^n$. Use Lemma 6.2 to find a representation $\psi : \mathbb{Z}_p^n \to \mathrm{GL}_d(\mathbb{C})$ such that $\rho(\varphi(x), \psi(x)) < p^{2n}\epsilon$. Since $\rho(\varphi(x), \mathrm{Id}) \geq \beta$ for all nonzero $x \in \mathbb{Z}_p^n$, it follows that for all $x \neq 0$

$$\rho(\psi(x), \mathrm{Id}) \geq \beta - p^{2n}\epsilon > \frac{p^n - p^{n-1}}{p^n - 1}.$$

This is a contradiction. □

Corollary 6.5. *The best constant for the class of all groups is* $1/2$.

6.1. The value of $\kappa(G)$ for finite groups

Let G be an arbitrary finite group. Note that it follows from Proposition 6.2 that

$$\kappa(G) = \sup_{\psi} \min_{g \in G} \rho(\psi(g), \mathrm{Id}),$$

where ψ ranges over all finite-dimensional representations of G. The first observation is that the supremum can be upgraded to a maximum.

Proposition 6.6. *Let G be a finite group. Then there exists a finite-dimensional representation $\psi : G \to \mathrm{GL}_d(\mathbb{C})$ of G such that*

$$\kappa(G) = \min_{g \in G} \rho(\psi(g), \mathrm{Id}).$$

In particular, $\kappa(G)$ is a rational number.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Proof. Denote by $R = \{\psi_0, \dots, \psi_{c-1}\}$ the set of all irreducible representations of G up to isomorphism. Pick $C = \{g_0, \dots, g_{c-1}\}$ to be a set of representatives for all conjugacy classes of G. We will assume that ψ_0 is the trivial representation and $g_0 := e$ is the identity element of G. Consider the $(c-1) \times (c-1)$ matrix K where

$$K_{ij} = \dim \ker (\psi_j(g_i) - \mathrm{Id}).$$

Note that K_{ij} does not depend on the choice of the representative g_i. Set $\beta = \kappa(G)$, and write

$$\Delta = \left\{ (x_1, \dots, x_{c-1}) : x_i \geq 0, \sum_{1 \leq i \leq c-1} x_i = 1 \right\}.$$

For each representation $\psi : G \to \mathrm{GL}_d(\mathbb{C})$ which does not contain the trivial representation, we can decompose ρ as $\rho = \oplus_{j=1}^{c-1} n_i \psi_i$, and define $\delta(\psi) \in \Delta$ to be the column vector:

$$\delta(\psi) = \left(\frac{n_1}{d}, \dots, \frac{n_{c-1}}{d} \right)^t,$$

of normalized multiplicities of irreducible representations of G. It is easy to see that $\min_{g \in G} \rho(\psi(g), \mathrm{Id}) \geq \alpha$ holds iff for all $g \in G$

$$\sum_{i=1}^{c-1} n_i \ker (\psi_i(g) - \mathrm{Id}) \leq (1 - \alpha) d.$$

These conditions can be more succinctly expressed as:

$$K\delta(\psi) \leq (1 - \alpha)(1, 1, \dots, 1)^t,$$

where we write $x \leq y$ for two vectors x, y if every entry of $y - x$ is nonnegative. By assumption, for every $m \geq 1$, there exists a representation ψ_m such that $K\delta(\psi_m) \leq (1 - \beta + \frac{1}{m})(1, 1, \dots, 1)^t$ holds. In other words, the set

$$\left\{ x \in \Delta : Kx \leq \left(1 - \beta + \frac{1}{m}\right)(1, 1, \dots, 1)^t \right\}$$

is nonempty. By compactness of Δ, it follows that there exists a point $x \in \Delta$ such that $Kx \leq (1 - \beta)(1, 1, \dots, 1)^t$. Note that these constitute a system of inequalities involving $x_1, \dots, x_{c-1}$ and β with rational coefficients. Now using the fact the the set of solutions to this system is a rational polytope (or equivalently using the proof of Farkas' lemma [16]), we deduce that both β and $(x_1, \dots, x_{c-1})$ are rational. This proves the claim. □

Remark 6.7. *There are noncyclic finite groups F for which $\kappa(F) = 1$. For instance, let F be a finite subgroup of $\mathrm{SU}_2(\mathbb{C})$. Such groups are cyclic of odd order and double covers of finite subgroups of $\mathrm{SO}_3(\mathbb{R})$, which include the alternating groups of 4, 5 letters, and the symmetric group on 4 letters. We claim that the natural representation ρ of F in $\mathrm{GL}_2(\mathbb{C})$ has the property that for $g \neq e$ the eigenvalues of $\rho(g)$ are not 1. This is clear since if one eigenvalue is 1, then the other has to be 1 as well, contradicting the faithfulness of ρ. These groups include, for instance, $\mathrm{SL}_2(\mathbb{F}_5)$.*

Proposition 6.8. *Let G be a finite group. Then $\kappa(G) = 1$ iff G has a fixed-point free complex representation.*

These groups have been classified by Joseph A. Wolf. The classification is rather complicated. We refer the reader to [24] for proofs and to [[17], Theorem (1.7)] for a concise statement and the table listing these groups. The difficulty of classifying finite groups G with $\kappa(G) = 1$ suggests that the problem of determining $\kappa(G)$ in terms of G may be a challenging one.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

Remark 6.9. *Given a field F, one can also study the notion of linear sofic approximation over F. It is not known whether linear sofic groups over $\mathbb{C}$ and other fields coincide. However, one can show that $\kappa_{\mathbb{C}}(G)$ and $\kappa_F(G)$ do not need to coincide. This will be seen in the next subsection.*

6.2. Optimal linear sofic approximation over fields of positive characteristic

In this subsection, we will prove Theorem C

Proof of Theorem C. Let F be a field of characteristic p. It is easy to see that the proof of Proposition 6.2 works over F without any changes. Hence, for any finite group G we have

$$\kappa_F(G) = \sup_{\psi} \min_{g \in G} \rho(\psi(g), \mathrm{Id}),$$

where ψ runs over all representations $\psi : G \to \mathrm{GL}_d(F)$.

Suppose $\rho: G \to \mathrm{GL}_d(F)$ is a linear representation. Let g be an element of order p in G. Write $\psi(g) = \mathrm{Id} + \tau(g)$ where $\tau(g)$ is a $d \times d$ matrix over F. From $\psi(g)^p = \mathrm{Id}$, and F has characteristic p, it follows that $\tau(g)^p = 0$. Let J denote the Jordan canonical form of $\tau(g)$, consisting of k blocks. It follows from $\tau(g)^p = 0$ that each block in J is a nilpotent block of size at most p, implying $kp \geq d$. Since $k = \dim \ker \tau(g)$, we have

$$\mathrm{rank}(\psi(g) - \mathrm{Id}) = d - \dim \ker \tau(g) \leq d - \frac{d}{p}.$$

This shows that $\kappa(G) \leq 1 - \frac{1}{p}$. To prove the reverse inequality, let V denote the vector space consisting of all functions $f : G \to F$. Clearly, $d := \dim V = |G|$. Consider the left regular representation of G on V defined by:

$$(\psi(g)f)(h) = f(gh).$$

Let $g \in G \setminus \{e\}$, and consider the subspace

$$W(g) = \{f \in V : \psi(g)f = f\}.$$

Any $f \in W(g)$ is invariant from the left by the subgroup $\langle g \rangle$ generated by g. It follows that

$$\dim W(g) \leq \frac{d}{|\langle g \rangle|} \leq \frac{d}{p}.$$

Hence,

$$\mathrm{rank}(\psi(g) - \mathrm{Id}) = d - \dim W(g) \geq d - \frac{d}{p},$$

proving the claim. □

Acknowledgment. The authors would like to thank Goulnara Arzhantseva for helpful comments and suggestions on an earlier version of this paper. We also thank the anonymous referee for a careful reading of the paper and numerous remarks that significantly improved the exposition of this paper. Special thanks are due to Iosif Pinelis for providing the reference to Theorem 3.2.

References

[1] G. Arzhantseva and P. A. Cherix, Quantifying metric approximations of discrete groups, *Ann. Fac. Sci. Toulouse Math*, Série 6, **33**(3) (2024), 831–877.
[2] G. Arzhantseva and L. Paunescu, Almost commuting permutations are near commuting permutations, *J. Funct. Anal.* **269**(3) (2015), 745–757. MR 3350728.
[3] G. Arzhantseva and L. Păunescu, Linear sofic groups and algebras, *Trans. Amer. Math. Soc.* **369**(4) (2017), 2285–2310.
[4] O. Becker and A. Lubotzky, Group stability and property (T), *J. Funct. Anal.* **278**(1) (2020), 108298. MR 4027744.
[5] O. Becker, A. Lubotzky and A. Thom, Stability and invariant random subgroups, *Duke Math. J.* **168**(12) (2019), 2207–2234. MR 3999445.
[6] M. De Chiffre, L. Glebsky, A. Lubotzky and A. Thom, Stability, cohomology vanishing, and nonapproximable groups, *Forum Math. Sigma.* **8**(e18) (2020), 37. MR 4080477.

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press

[7] G. Elek and Ł. Grabowski, Almost commuting matrices with respect to the rank metric, *Groups Geom. Dyn.* **15**(3) (2021), 1059–1083. MR 4322021.
[8] G. Elek and E. Szabó, Hyperlinearity, essentially free actions and L^2-invariants, the sofic property, *Math. Ann.* **332**(2) (2005), 421–441. MR 2178069.
[9] C. G. Esseen, On the Kolmogorov-Rogozin inequality for the concentration function, *Z. Wahrscheinlichkeitstheorie Und Verw. Gebiete* **5**(3) (1966), 210–216. MR 205297.
[10] L. Glebsky and L. M. Rivera, Almost solutions of equations in permutations, *Taiwanese J. Math.* **13**(2A) (2009), 493–500. MR 2500002.
[11] M. Gromov, Endomorphisms of symbolic algebraic varieties, *J. Eur. Math. Soc. (JEMS)* **1**(2) (1999), 109–197. MR 1694588.
[12] K. Iima and R. Iwamatsu, On the Jordan decomposition of tensored matrices of Jordan canonical forms, *Math. J. Okayama Univ.* **51** (2009), 133–148. MR 2482411.
[13] A. Kolmogorov, Sur les propriétés des fonctions de concentrations de M. P. Lévy. *Ann. Inst. H. Poincaré* **16** (1958), 27–34. MR 101545.
[14] B Luong, Fourier analysis on finite abelian groups, *Applied and Numerical Harmonic Analysis* (Birkhäuser Boston, Ltd, Boston, MA, 2009). MR 2537697.
[15] K. Maples, Singularity of random matrices over finite fields, 2010. https://arxiv.org/abs/1012.2372
[16] J. Matousek, *Understanding and using linear programming* (Springer, Berlin, 2007).
[17] M. Nakaoka, Finite groups which act freely on spheres, *Osaka Math. J.* **11** (1974), 323–330. MR 356108.
[18] H. H. Nguyen and M. M. Wood, Random integral matrices: universality of surjectivity and the cokernel, *Invent. Math.* **228** (1) (2022), 1–76.
[19] V. V. Petrov, Ergebnisse der Mathematik und ihrer Grenzgebiete, *Sums of independent random variables* (Springer-Verlag, New York-Heidelberg, 1975). Band 82, Translated from the Russian by A. A. Brown. MR 0388499
[20] B. A. Rogozin, An estimate of the concentration functions, *Teor. Verojatnost. i Primenen* **6** (1961), 103–105. MR 0131893.
[21] F. Rădulescu, The von Neumann algebra of the non-residually finite Baumslag group embeds into, Hot topics in operator theory, *Theta Ser. Adv. Math*, vol. **9** (Theta, Bucharest, 2008), 173–185. MR 2436761.
[22] T. Tao and V. Van, *Additive combinatorics* (Cambridge University Press, Cambridge, 2006)
[23] B. Weiss, Sofic groups and dynamical systems, Ergodic theory and harmonic analysis, **62** (2000), 350–359. (Mumbai, 1999) MR 1803462
[24] J. A. Wolf, *Spaces of constant curvature* (McGraw-Hill Book Co, New York-London-Sydney, 1967). MR 0217740

https://doi.org/10.1017/S0017089524000351 Published online by Cambridge University Press